ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение высшего профессионального образования
«Уральский государственный университет им. А.М. Горького»

ИОНЦ «Информационная безопасность»

математико-механический факультет

кафедра алгебры и дискретной математики

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС
«Библиотека для модулярной целой арифметики и арифметики в конечных полях»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ КОМПЛЕКСА

Автор: ведущий математик РУНЦ
«Информационная безопасность»
Ю. С. Лукач

Екатеринбург
2007

ВВЕДЕНИЕ

Учебно-методический комплекс «Библиотека для модулярной целой арифметики и арифметики в конечных полях», далее именуемый УМК, является составной частью более общего учебно-методического комплекса «Библиотека Marwin для целой, рациональной и полиномиальной арифметики произвольной точности под ОС Windows».

Основанием для разработки такой библиотеки послужили следующие соображения. Существующие библиотеки арифметики произвольной точности (GNU MP, Pari, CLN и др.) неудобны для использования в учебном процессе по целому ряду причин. Во-первых, их исходный код ориентирован на профессиональных разработчиков и очень труден для понимания студентами. Во-вторых, все подобные библиотеки разработаны для операционной систем семейства UNIX и плохо переносятся в ОС Windows, которая на сегодня является основной операционной средой, в которой обучаются студенты нашего университета.

Вместе с тем назрела настоятельная необходимость в удобном инструментарии для проведения быстрых арифметических вычислений в числовых кольцах, прежде всего, в кольцах $\boldsymbol{Z}$ (целые числа), $\boldsymbol{Z(m)}$ (кольца вычетов по модулю $\boldsymbol{m}$), $\boldsymbol{Q}$ (рациональные числа) и $\boldsymbol{GF(p^n)}$ (конечные поля), а также в кольцах полиномов над указанными кольцами. Необходимость в таком инструментарии диктуется потребностями сразу нескольких учебных дисциплин и научно-исследовательских направлений математико-механического факультета. Среди них можно выделить вычислительную математику, математическое моделирование, алгоритмическую теорию чисел, компьютерную алгебру, криптографию и защиту информации.

Все эти соображения привели к тому, что автором была начата разработка собственной библиотеки на языке C++, реализующая все перечисленные потребности. Дополнительными требованиями при разработке библиотеки были следующие.

- Библиотека должна функционировать в среде Windows и поддерживать основные аппаратные архитектуры, на которых реализована данная среда, а именно: IA-32/x86 (Pentium 4), IA-32/x64 (AMD-64) и IA-64 (Itanium 2).
- Библиотека должна быть написана прозрачным и ясным кодом на языке C++ с тем, чтобы студенты могли легко ей пользоваться и по мере необходимости добавлять к ней свои реализации различных алгоритмов и тестировать их.
- Вместе с тем реализация вычислений в библиотеке должна быть достаточно эффективной с тем, чтобы обеспечить решение реальных задач, возникающих в перечисленных выше областях компьютерной математики.

СОСТАВ УМК

В состав УМК входят библиотека Marwin версии 1.1, ее описание, демонстрационные программы и некоторые итоги тестов.

В данной версии библиотеки реализованы:

- целочисленная арифметика произвольной точности;
- рациональная арифметика произвольной точности;
- модулярная арифметика произвольной точности;
- генератор псевдослучайных чисел произвольной длины;
- базовый набор комбинаторных функций (вычисление факториала, биномиальных коэффициентов, чисел Фибоначчи и Лукаса);
- базовый набор теоретико-числовых функций (вероятностные тесты простоты чисел, символы Якоби, Лежандра и Кронекера).

Проведенные тесты показали, что вычисления в библиотеке Marwin производятся быстрее в сравнении с аналогичными по возможностям библиотекам в 3–10 раз. Это относится как к библиотекам с открытым исходным кодом (GNU MP, Pari, CLN), так и к коммерческим пакетам (Maple, Mathematica). Такое быстродействие достигнуто благодаря сочетанию трех факторов.

- Тщательный отбор использованных алгоритмов и их скрупулезное программирование.
- Ручная оптимизация ядра библиотеки путем переписывания критических по времени частей на языке ассемблера.
- Оптимизированное для ОС Windows управление динамической памятью.

Перечислим основные алгоритмы, реализованные в ядре библиотеки Marwin.

Умножение целых чисел в зависимости от длины операндов производится одним из следующих алгоритмов: умножение «в столбик», алгоритм Карацубы, алгоритм Тоома-Кука 3x3, быстрое преобразование Фурье методом Шёнхаге-Штрассена.

Деление целых чисел с остатком производится рекурсивным методом Бурникеля-Зиглера. Для деления нацело не слишком больших чисел используется ускоренный алгоритм Йебелеана.

Вычисление наибольшего общего делителя (НОД) производится в зависимости от длины операндов либо алгоритмом Вебера, либо алгоритмом Шёнхаге. Обобщенный НОД (т. е. НОД и сопутствующие сомножители) вычисляются либо алгоритмом Лемера, либо алгоритмом Шёнхаге.

Модулярная арифметика также имеет несколько вариантов в зависимости от длины и строения модуля. Для модулей вида 2^n и $2^n \pm 1$ используется 2-

адическая арифметика. Для очень коротких и очень длинных нечетных модулей числа представляются в форме Монтгомери, позволяющей использовать его алгоритм REDC. В остальных случаях используется обычная целая арифметика с вычислением остатков по данному модулю.

СТРУКТУРА БИБЛИОТЕКИ И ЕЕ ИСПОЛЬЗОВАНИЕ

Библиотека Marwin построена по модульному принципу и состоит из ядра и библиотеки классов. Ядро разработано в двух вариантах: «generic» ядро, которое написано на чистом языке C++ без использования ассемблера и может быть скомпилировано для любой платформы, и оптимизированные ядра с ассемблерными вставками для платформ Pentium 4, AMD-64 и Itanium 2. В библиотеку версии 1.1 включены два ядра – для произвольных процессоров Pentium и для процессора Pentium 4. 64-битные версии ядра в настоящее время находятся на стадии тестирования.

С точки зрения пользователя Marwin представляет собой обычную библиотеку классов на языке C++, которая предоставляет возможности, перечисленные в предыдущем разделе. Все сложности ядра от пользователя скрыты, поэтому для пользования библиотекой не нужно знать тонкости реализации той или иной операции.

Дистрибутивный диск имеет следующую структуру папок:

- BIN – динамические библиотеки и исполняемые файлы примеров.
- DATA – результаты тестовых прогонов, показывающие скорость основных операций.
- DEMO – исходные тексты примеров.
- DOC – руководство пользователя, содержащее детальное описание классов библиотеки, в форматах CHM и PDF.
- INCLUDE – заголовочные файлы библиотеки.
- LIB – библиотечные файлы для компоновки программ.

Файлы библиотеки и примеров представлены в нескольких вариантах в зависимости от ядра и использованного компилятора C++, а именно:

MARWIN_GEN_I.DLL – ядро «generic», компилятор Intel;
MARWIN_GEN_MS.DLL – ядро «generic», компилятор Microsoft;
MARWIN_X86_I.DLL – ядро Pentium 4, компилятор Intel;
MARWIN_X86_MS.DLL – ядро Pentium 4, компилятор Microsoft.

Аналогичным образом называются соответствующие библиотечные файлы и исполняемые файлы примеров.

Для просмотра данных из папки DATA в виде графиков требуется программа GNUPLOT, которую можно бесплатно скачать по адресу http://www.gnuplot.info.

Для пользования библиотекой Marwin необходимо выполнить следующие действия.

- Скопировать нужные вам файлы с расширением .DLL из папки BIN в системную папку или любую другую папку Windows, включенную в переменную окружения PATH.
- В начало своей программы на языке C++ добавить директивы, подключающие заголовочный файл библиотеки MARWIN.H из папки INCLUDE (см. примеры в папке DEMO).
- Указать компоновщику, что вашу программу необходимо компоновать с одной из библиотек MARWIN_xxx_yy.LIB из папки LIB.

Замечания, сообщения об ошибках и предложения по улучшению функциональности библиотеки просим направлять разработчику по адресу yl@suncloud.ru.